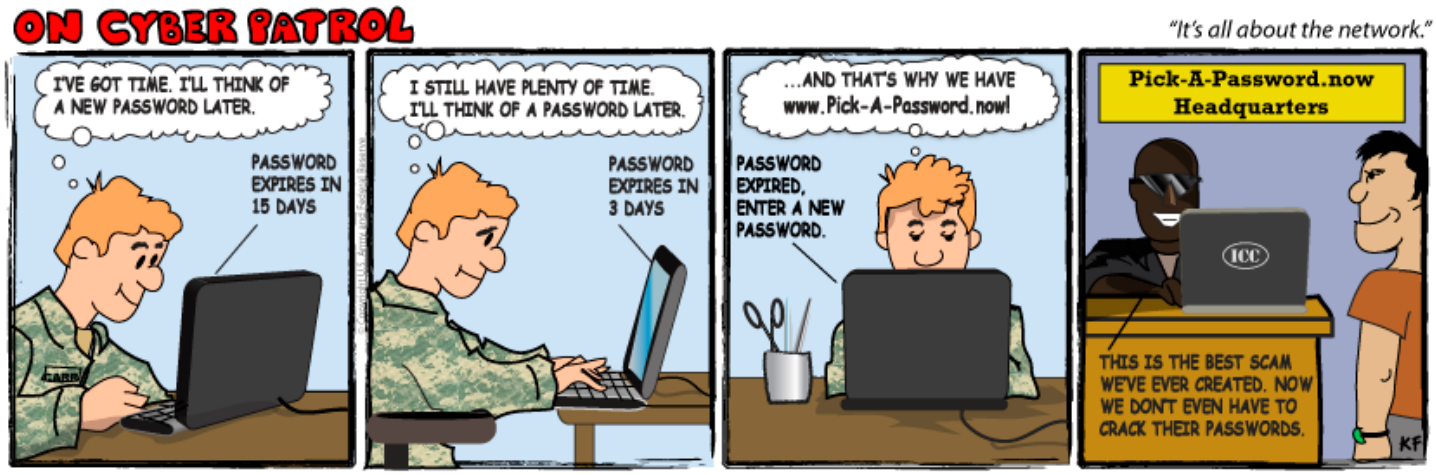
Password Protected

September 2012



Password Policies - The Key to a Secure System

We often find ourselves receiving notices that our password is about to expire and needs to be changed. Many times we curse getting that message because we have so many other things to worry about that require our immediate attention, and we know the time and frustration that results from having to think of and remember a new password. Additionally, most of us have passwords to our many personal accounts from email, to banking, to social media accounts that we must remember. However, we must not forget how important having a strong password is to ensure that not only our personal information is safeguarded, but the official government systems we use are also protected.

Passwords are used to ensure that only authorized personnel are granted access to information. It is the user's responsibility to ensure that the password they create is both easy enough to remember without being written down, and is also not easy for someone else to guess.

Many organizations have password policies detailing password construction in order to reduce the likelihood of unauthorized access. A poorly chosen password may be easy to figure out and could lead to unauthorized access and exploitation of organization resources. It is the user's responsibility to protect the password once it has been chosen. Passwords should never be written down and hidden under keyboards, monitors, or desk. Passwords should be constructed so the user can remember them without the need for them to be written down.

Many users assign passwords based on things in their personal life, such as spouse's name, name of the family pet, or their children's birthday. In these days of social media it is not difficult to find out the birthday of a child or the name of a pet. Someone that is determined can research social media sites to find out key information about your personal life. Many people post pictures from birthday parties, graduation photos and other significant events which provide useful information to would be hackers. Users should ensure they refrain from using personal information as passwords even if they assume no one will guess that information. A password like 'DUKE1992!!' may seem like a safe password to assign to your system initially. The careful listener may have overheard you mention you attended Duke during one of their National Championship years. With that information it may only take a few attempts to gain access to a system.

A strong password should contain 8-14 characters and at least three of the five following characteristics:
-Upper case characters
-Lower case characters
-Punctuations
-Numbers
-Special characters (&%$@#)

Additionally, passwords are considered weak if any of the following are true:
-contains a word found in the dictionary
-word or number patterns (abcde, 12345, 112233)
-organization or company name (acme, acme1, acmeNY, payroll)
-recently used passwords

Users should consider using a passphrase instead of a password. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

An example of a passphrase is 'Mi2c0mputas@h0me' which has the same characteristics of a good password.

At the end of the day it is the user's responsibility to create a strong password in accordance with the organization's password policy and to safeguard that password so it does not fall into the wrong hands. It is of equally importance to guard your work password as it is to guard the password to your personal accounts because we must all be good stewards of the network.